

US009519771B2

(12) United States Patent

Fadell et al.

(54) EMBEDDED AUTHENTICATION SYSTEMS IN AN ELECTRONIC DEVICE

(71) Applicant: Apple Inc., Cupertino, CA (US)

(72) Inventors: **Anthony Fadell**, Portola Valley, CA (US); **Andrew Hodge**, Palo Alto, CA

(US); Stephan Schell, Cupertino, CA (US); Ruben Caballero, San Jose, CA (US); Jesse Lee Dorogusker, Los Altos, CA (US); Stephen Zadesky, Portola Valley, CA (US); Emery

Sanford, San Francisco, CA (US)

(73) Assignee: Apple Inc., Cupertino, CA (US)

(*) Notice: Subject to any disclaimer, the term of this

patent is extended or adjusted under 35

U.S.C. 154(b) by 0 days.

(21) Appl. No.: 14/142,669

(22) Filed: Dec. 27, 2013

(65) **Prior Publication Data**

US 2014/0115695 A1 Apr. 24, 2014

Related U.S. Application Data

(63) Continuation of application No. 12/207,374, filed on Sep. 9, 2008, now Pat. No. 8,943,580. (Continued)

(51) Int. Cl. *G06F 7/04 G06F 21/36*

(2006.01) (2013.01)

(Continued)

(52) U.S. Cl.

(Continued)

(58) Field of Classification Search

CPC G06F 21/32; G06F 3/0412; G06F 3/0416; G06F 3/04817; G06F 3/0488; G06F 3/04883; G06F 21/316; H04L (10) Patent No.: US 9,519,771 B2

(45) **Date of Patent:**

Dec. 13, 2016

63/0861; G06K 9/0002; G06K 9/00033; G06K 9/0013; G06K 9/00087; G06K 9/00912

(Continued)

(56) References Cited

U.S. PATENT DOCUMENTS

4,353,056 A 10/1982 Tsikos 4,993,068 A 2/1991 Piosenka et al. (Continued)

FOREIGN PATENT DOCUMENTS

CN 1220433 A 6/1999 CN 1685357 A 10/2005 (Continued)

OTHER PUBLICATIONS

Notice of Allowance received for U.S. Appl. No. 11/322,550, mailed on Sep. 19, 2008, 12 pages.

(Continued)

Primary Examiner — Techane Gergiso (74) Attorney, Agent, or Firm — Morrison & Foerster LLP

(57) ABSTRACT

This invention is directed to an electronic device with an embedded authentication system for restricting access to device resources. The authentication system may include one or more sensors operative to detect biometric information of a user. The sensors may be positioned in the device such that the sensors may detect appropriate biometric information as the user operates the device, without requiring the user to perform a step for providing the biometric information (e.g., embedding a fingerprint sensor in an input mechanism instead of providing a fingerprint sensor in a separate part of the device housing). In some embodiments, the authentication system may be operative to detect a visual or temporal pattern of inputs to authenticate a user. In response to authenticating, a user may access restricted files, applications (e.g., applications purchased by the user), or settings (e.g., application settings such as contacts or saved game profile).

33 Claims, 10 Drawing Sheets

